CYBERIUM ARENA

## Descripción

Este programa de Operación SOC está diseñado para que las organizaciones SOC implementen una solución SOC y proporcionen una guía completa sobre las habilidades y procedimientos necesarios para operarla. El programa brinda a los participantes todos los aspectos de un equipo SOC para mantener a raya al adversario de la empresa.

# NX220 - ANALISTA SOC

### Módulo 1: Dominio de Windows

Este módulo enfocado se centra en Sysmon, una potente herramienta de monitoreo del sistema Windows. Enseña a los aprendices cómo usar Sysmon para un registro de eventos comprensivo, contribuyendo a una comprensión más profunda de las operaciones del dominio de Windows.

**Servidor Windows**
Instalación de Servidor Windows
Configuración de Servidor Windows
Gestión de Características
Eventos de Windows
Sysmon
**Dominio de Windows**
Instalación de AD DS
Configuración de AD DS
Gestión de Protocolos de Dominio
Trabajando con Política de Grupo
Trabajando con Wireshark

### Módulo 2: Entorno SOC

Este módulo incluye la configuración y gestión de Firewalls usando pfSense, incluyendo la creación de reglas de firewall y NAT. Involucra monitoreo del sistema en tiempo real y explora Sistemas de Detección y Prevención de Intrusiones (IDS/IPS). Los participantes ganan experiencia práctica con Snort, entendiendo estructuras de reglas, configuración y análisis de tráfico avanzado usando la característica NAT.

**Firewalls**
Instalación de pfSense
Configuración de Reglas FW
Configuración de Reglas NAT
Instalación y Gestión de Paquetes
Monitoreo en Tiempo Real
**IDS/IPS**
Trabajando con Snort
Estructura de Reglas de Snort
Configuración y Establecimiento de Reglas
Pasando Tráfico usando la Característica NAT
Análisis de Reglas Avanzadas

### Módulo 3: Uso del SIEM

Este módulo guía a los participantes a través de los componentes esenciales de la Gestión de Información y Eventos de Seguridad (SIEM). Se inicia con la exploración de la pila ELK, cubriendo monitoreo de eventos, métodos de búsqueda, consultas personalizadas y configuraciones de alertas. La parte final profundiza en Splunk, enseñando cómo monitorear eventos, los fundamentos del Lenguaje de Procesamiento de Búsqueda (SPL).

**ELK**
Monitoreo de Eventos
Métodos de Búsqueda Diferentes
Consultas Personalizadas
Configuración de Alertas
**Splunk**
Monitoreo con Splunk
Alertas de Splunk

### Módulo 4: Caza de Amenazas

Este módulo sumerge a los participantes en aspectos avanzados de la ciberseguridad. Comienza con un análisis de logs comprensivo, incorporando filtrado avanzado y caza de amenazas a través de eventos y MITRE ATT&CK. Los participantes trabajan con Sysmon y su configuración, seguido por explorar YARA para la creación de reglas y caza de amenazas.

**Análisis de Logs**
Análisis de Logs
Filtrado Avanzado
**MITRE ATT&CK**
Caza a través de Eventos
Creación de Reglas de Caza
**Sysmon**
Configuración de Ajustes XML
Análisis de Eventos de Sysmon
**YARA**
Estructura de Reglas
Caza con YARA
**Respuesta a Incidentes**
Playbooks de IR
Investigación de Archivos

**Defensa NX | NIVEL: 3 | DURACIÓN: 10-12 semanas (autoaprendizaje) / 40h (con instructor)**